

FILED: October 9, 2019

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 18-4302
(1:17-cr-00302-LMB-1)

UNITED STATES OF AMERICA,

Plaintiff – Appellee,

v.

NIKOLAI BOSYK,

Defendant – Appellant.

ELECTRONIC FRONTIER FOUNDATION,

Amicus Supporting Appellant.

ORDER

The court denies the petition for rehearing en banc.

A requested poll of the court failed to produce a majority of judges in regular active service and not disqualified who voted in favor of rehearing en banc. Chief Judge Gregory, Judge Wilkinson, Judge Niemeyer, Judge Motz, Judge King, Judge Agee, Judge Keenan, Judge Diaz, Judge Floyd, Judge Thacker, Judge Harris, Judge Richardson, Judge

Quattlebaum, and Judge Rushing voted to deny rehearing en banc. Judge Wynn voted to grant rehearing en banc and filed a separate statement.

Entered at the direction of Judge Diaz.

For the Court

/s/ Patricia S. Connor, Clerk

WYNN, Circuit Judge, statement in the denial of rehearing en banc:

The Government in this matter leads this Court to depart from the wisdom of our sister circuits and endorse an unsustainable approach to evaluating evolving technology. At the core of this matter is the Government's affidavit which states that someone using Defendant's IP address was in the wrong place at a certain time. Not at the wrong time—just at a certain time.

As I discussed in my dissent, reasoning by analogy depends on relevant similarity. To many courts, the internet is abstract and the task of learning what a URL is—or what a dynamic URL is, or what a URL shortener does, and what the implications may be—represents a specialized undertaking unrelated to legal expertise, that is, something to approach with a sense of dread. Tools like analogies that promise to reduce a technical issue to something susceptible to the intuitive logic of the familiar become appealing. And retrospective confirmation, such as when we can look back and see that an affidavit led to a computer filled with child pornography, builds trust that the logic that found probable cause was sound in the first instance. However, legal commentators have raised the alarm about indiscriminate use of metaphors in the internet context. *See, e.g.*, Mark A. Lemley, *Place and Cyberspace*, 91 Calif. L. Rev. 521, 542 (2003) (“The cyberspace as place metaphor can be valuable . . . [but t]he metaphor will serve its purpose only if we understand its limitations—the ways in which the Internet is not like the physical world.”). Sometimes, the preference to avoid taking the internet on its own terms, to avoid learning new rules and starting from logical scratch, leads us to not question basic assumptions when we should. This is one of those cases.

I offer a comparison of two analogies to illustrate the problem. Both start with what seems like a reasonable general metaphor that describes how a human user experiences the internet. After that point, however, based on the initial choice of metaphor, each analogy naturally takes a different path, and the two analogies ultimately suggest opposing conclusions. Both conclusions are “right” according to their analogy’s logic. But by the time they reach those conclusions, both analogies have become somewhat divorced from reality and in neither case can we go back and “check our work” without reference to the technology that we are trying to describe.

In the first analogy, we begin in a building. This building is the confines of the internet. We are standing in a room and this room is a section of an internet forum, Bulletin Board A. We see a door with a sign that advertises child pornography. The door is the download link URL that was posted on Bulletin Board A. We open that door and encounter both a cache of child pornography and the Defendant. If we believe the door we used was the only door to that place—indeed, so long as the number of doors into the room is a manageable number, or so long as we speculate on the basis of proximity that only places like Bulletin Board A have doors that lead here—we can reasonably conclude that Defendant is seeking child pornography.

In the second analogy, we begin on a field. That field is the vastness of the internet. The general area where we are standing is Bulletin Board A. We see a sign that points in a direction and advertises child pornography. That sign is the link posted on Bulletin Board A. We follow the sign’s instructions and eventually reach a place, where there is a cache of child pornography on the ground. We also encounter Defendant in the immediate

vicinity, but we did not see where he came from. Because there are no walls in this environment to direct traffic, we cannot reasonably conclude that Defendant, like us, followed the sign advertising child pornography.

This second analogy does not seek to explain the internet, rather, it seeks to explain how a foundational fault in the Government's logic skewed the Government's conclusion. The Government, the magistrate judge, the district court, and the majority in this case read the affidavit using an inapplicable logic of enclosure. They assumed limitations—represented by walls—that do not exist online. That said, the field analogy is also misleading in its own way. The field's openness suggests that we can and do see exactly where a link will take us, which, as the *amicus curiae* in this case explained, is not the case. The field analogy also risks spiraling into a detailed and unhelpful geography if used to explain the role of the File Sharing Site. Every analogy can only go so far. This is why courts depend on *amici curiae* and, more importantly, the parties themselves, to explain technical issues in cases like this one, and to explain them well. *See, e.g., In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 306 n.1 (3d Cir. 2010) (thanking a group of *amici* led by the Electronic Frontier Foundation for participating in a case involving an *ex parte* application by the government and an issue of first impression related to the Stored Communications Act and cell site location information).

Examining the affidavit in this case, it is technological error to conclude that “the records showed that . . . someone using this IP address clicked *that same link*.” *United States v. Bosyk*, 933 F.3d 319, 323 (4th Cir. 2019) (emphasis added). Indeed, the affidavit

does not make this direct causal allegation. The affidavit represented that some number of hours before or some number of hours after some anonymous actor posted *a certain* link on *a certain* website, someone using Defendant's IP address came into contact with *some* link that was perhaps found on *some* website.

The affidavit does not say that the Defendant's IP address had ever been associated with any child pornography activity in the past. The affidavit does not say the person using Defendant's IP address actually downloaded any of the password-protected files. The affidavit does not even say that the person with Defendant's IP address arrived at the URL in question after the suspect link was posted on the monitored website—a bar so low that it is alarming that the affidavit tripped over it. We know from other cases in other circuits that such facts are relevant to finding probable cause. *See, e.g., United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006). These kinds of facts, however, are all missing here.

In the digital age, the ubiquity of link shortening services and randomly generated URLs renders browsing the Internet a great exercise in trusting strangers. The average internet user does not—indeed, cannot—know with certainty that all the links they follow will take them where they expect. The system works because we follow links on faith. What, then, should a court assume when an affidavit alleges nothing more than that a single click occurred? Very little, if anything.